

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of)
(Briefly describe the property to be searched)
or identify the person by name and address)) Case No. 20-1046M(NJ)
information associated with two Apple)
ID's/iCloud accounts that is stored at premises)
controlled by Apple)

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the _____ District of _____

(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

YOU ARE COMMANDED to execute this warrant on or before October 21, 2020 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10:00 p.m. ☒ at any time in the day or night because good cause has been established.

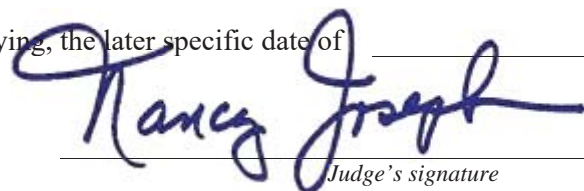
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Hon. Nancy Joseph.

(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: October 7, 2020


Judge's signature

City and state: Milwaukee, Wisconsin

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

Return

Case No.:

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name(s) of any person(s) seized:

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

Executing officer's signature

Printed name and title

ATTACHMENT A

Matter No. 2020R00324

Property to Be Searched

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

Account 1:

- Name: Tyler Vaughn
- Email: dtv2017@icloud.com
- Phone: (262) 234-1468
- Person ID: 17412011338
- Addresses: 327 Kenzie Ave. Racine, WI 53405

Account 2:

- Name: Dev Vaughn
- Email: dtvon@icloud.com
- Phone: (262) 234-1468
- Person ID: 17429487926
- Address: 925 Author Ave. Racine, WI 53405

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers

(“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from August 23, 2020 through the date this warrant issued, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August 23, 2020 through the date this warrant issued, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all

address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of arson of commercial property, in violation of Title 18, United States Code, Section 844, involving Devon Vaughn since August 23, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Preparatory steps taken in furtherance of these crimes;
- b. Communications between Devon Vaughn and Tabitha Scruggs;
- c. Information about the protests, riots, and civil unrest in the Kenosha, Wisconsin area occurring between August 23, 2020 and the date this warrant issued;
- d. Use, possession, custody, or control of the phone numbers (262) 676-9514 and (262) 234-1468;
- e. Accelerants or ignitable liquids (such as gasoline, kerosene, or other petroleum distillates), glass bottles, ignition devices (such as an improvised wick or towel), heat sources, and ignition sources (such as a lighter or matches);
- f. Appearance, clothing, and identity of Devon Vaughn on August 24, 2020;
- g. B & L Office Furniture, located 1101 60th St. Kenosha, WI;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Any information related to motive, intent, or knowledge of the violations described above;
- j. Any information related to the concealment or destruction of evidence of the violations described above;
- k. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

- m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and
- n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

UNITED STATES DISTRICT COURT

for the
Eastern District of Wisconsin

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)

information associated with two Apple ID's/iCloud
accounts that is stored at premises controlled by Apple

Case No
20-1046M(NJ)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A

located in the _____ District of _____, there is now concealed (identify the person or describe the property to be seized):

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☐ contraband, fruits of crime, or other items illegally possessed;
☐ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section
Title 18, U.S.C., Sections 844 arson

Offense Description

The application is based on these facts:
See the attached affidavit.

- ☒ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.



Applicant's signature

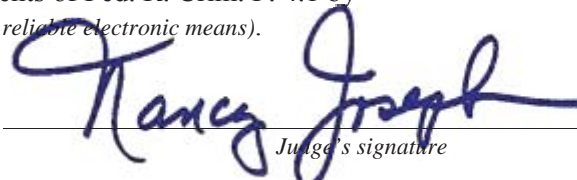
ATF SA Jody Keeku

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by
_____ telephone _____ (specify reliable electronic means).

Date: 10/7/20 _____

City and state: Milwaukee,
Wisconsin



Judge's signature

Hon. Nancy Joseph, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

Matter No. 2020R00324

I, Jody Keeku, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the Apple IDs and Apple iCloud accounts associated with the following information, further described in Attachment A, that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at One Apple Park Way, Cupertino, California 95014:

Account 1:

- Name: Tyler Vaughn
- Email: dtv2017@icloud.com
- Phone: (262) 234-1468
- Person ID: 17412011338
- Addresses: 327 Kenzie Ave. Racine, WI 53405

Account 2:

- Name: Dev Vaughn
- Email: dtvon@icloud.com
- Phone: (262) 234-1468
- Person ID: 17429487926
- Address: 925 Author Ave. Racine, WI 53405

2. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

3. I am a Special Agent of the United States Justice Department, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), currently assigned to the Milwaukee Field Office. I

have been so employed since July 2001. My duties as a Special Agent with ATF include investigating alleged violations of the federal firearms, explosives, and arson statutes.

4. I have completed approximately 26 weeks of training at the Federal Law Enforcement Training Center (Glynco, Georgia), as well as the ATF National Academy. That training included various legal courses related to Constitutional Law as well as search and seizure authority. Additionally, I have received training on how to conduct various tasks associated with criminal investigations, such as: interviewing, surveillance, and evidence collection.

5. In addition to my duties as a criminal investigator, I am also an ATF Certified Explosive Specialist Bomb Technician (CESBT). As a CESBT I conduct post-blast investigations in the Chicago Field Division and other ATF Jurisdictions as assigned, provide technical assistance to state/local bomb squads and other ATF agents in the investigation of explosions; provide safe disposal of recovered, purchased, seized or forfeited explosive materials; provide explosive diagnostic capabilities at special events. I have participated in the scene examination and post-blast investigation of over 10 explosive related activities. I have coordinated, instructed and participated in over eight live explosive training scenarios for post blast investigation training. I have also participated as an assistant instructor at the Advanced Explosive Disposal Techniques course and I have conducted or participated in several explosive disposal operations. As a Bomb Technician, I am responsible for conducting investigations, render safe, disassembly, and/or disposal of suspected hazardous device(s), explosives, explosive materials, pyrotechnics and ammunition. Responsibilities also include coordination with other local, state, and federal partners to investigate, perform diagnostics and potential render safe operations in chemical, biological, radiological, nuclear, and explosive (CBRNE) events. I conduct bombing crime scene investigations, collect and preserve evidence, and prepare and provide courtroom testimony. I

maintain issued bomb squad equipment, provide technical support to special operations, and provide dignitary protection. I have prepared and participated in explosive related training, and am familiar with technical and intelligence publications, the federal explosives laws and regulations and other explosive related materials. I maintain professional training and liaison with other public safety bomb squads, explosive detection canine units, special weapons and tactics (SWAT) units, military EOD units, federal agencies and professional associations such as IABTI. I report investigative and technical data on explosives related incidents and activities to the Bomb and Arson Tracking System (BATS).

6. Through my experience and training as a firearm, arson, and explosives investigator, I am aware that social media sites, such as Facebook, can be used to store and save audio, video, and text files that can link to a variety of criminal activity. I am also aware that social media sites, such as Facebook, are often used by witnesses to crime to record criminal activity.

7. I have previously applied for and received search and arrest warrants related to the crime of arson, as well as other crimes.

8. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

9. Based on the facts as set forth in this affidavit, there is probable cause to believe that the information described in Attachment A contains evidence of a violation of Title 18, United States Code, Section 844 (arson), as described in Attachment B.

JURISDICTION

10. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

11. On August 23, 2020, Jacob Blake was shot multiple times by officers of the Kenosha Police Department. That incident triggered both non-violent protests and violent rioting, including numerous arsons throughout the City of Kenosha. The unrest and violence grew so dangerous that the Wisconsin National Guard eventually deployed over 1,000 individuals to keep the peace. The Government also marshaled its resources to investigate crimes in the aftermath.

12. ATF’s National Response Team (NRT) and the Milwaukee Field Office, in partnership with the Kenosha Police Department, Kenosha Fire Department, Kenosha Sheriff’s Office, Drug Enforcement Administration, Wisconsin Department of Justice’s Division of Criminal Investigation, and the United States Attorney’s Office are focusing their efforts on identifying the persons responsible for twenty building arsons, seven vehicle arsons, and other related crimes that occurred in Kenosha between Sunday, August 23, 2020 and Tuesday, August 25, 2020. Those investigators processed scenes, collected video evidence, and identified potential witnesses, subjects, and targets. The instant warrant application is made as a part of this same investigative effort.

13. In conjunction with other federal, state, and local law enforcement officers, I am assisting with an investigation into an arson at B&L Office Furniture, located at 1101 60th Street,

in Kenosha, Wisconsin (“B&L”), on August 24, 2020. As part of the investigation into this arson at B&L, law enforcement reviewed a video publicly posted on the social media platform Twitter, which depicted a white male subject (wearing a black baseball cap, black tank top, blue surgical mask, and bearing a large left forearm tattoo, which itself featured a distinctive “straight edge” on the top) lighting a piece of material (believed to be either paper or cardboard) on fire, placing that same burning material on a table in front of B&L, and leaving the area.

14. Law enforcement located additional footage of a person matching the description of the white male mentioned above, also generated in Kenosha on the evening of August 24, 2020. A still image generated using this same footage was released to the media, and citizens with any knowledge of this person’s identity were asked to contact law enforcement at an established “tip line.”

15. A citizen who wished to remain anonymous (“CW No. 1”) contacted this “tip line” and advised that his son (“CW No. 2”), who also wished to remain anonymous, was familiar with the white male described above. CW No. 1 explained that CW No. 2 was connected on Facebook and Snapchat with a woman (later identified as Tabitha Scruggs [“Scruggs”]) whose boyfriend matched the picture released to the media. Law enforcement interviewed CW No. 2, at which point CW No. 2 (i) explained that Scruggs’ Facebook profile name was “Tabby Abby”; and (ii) provided a still photo associated with that same Facebook profile, which depicted Scruggs’ boyfriend Devon Vaughn (“Vaughn”). In the picture, Vaughn is wearing the same hat as the B&L arsonist and displays a tattoo on his left forearm with a straight edge in the same location as the B&L arsonist.

16. On September 3, 2020, law enforcement interviewed Scruggs outside of 3827 Republic Avenue in Kenosha, WI. This is the residence of Scruggs' grandmother, Eileen Scruggs ("Eileen").

17. Eileen initially answered the door, at which point law enforcement asked if "Tabitha" lived at the residence. Eileen responded that they had just missed her. Eileen eventually offered to call Scruggs. This call was placed, and Scruggs arranged to return to the residence.

18. While waiting for Scruggs to return, law enforcement asked Eileen if she knew of Scruggs' boyfriend. Eileen said she did, and his name was Devon.

19. Law enforcement showed Eileen a picture of Devon, from Scruggs' Facebook account, and asked Eileen if that was Devon, Scruggs' boyfriend. Eileen said it was.

20. When Scruggs returned to the residence, law enforcement interviewed her. Initially Scruggs stated she went to downtown Kenosha by herself, but she eventually acknowledged going downtown with her friend Devon. Scruggs claimed she did not know Devon's last name or cell phone number. Scruggs stated she had known Devon for three months and that they had originally met through Facebook.

21. Scruggs stated that Devon drove her, using her vehicle, to downtown Kenosha during the night of "the shooting" in Kenosha. She further stated that Devon continuously left her while they were downtown, and she was not around him for a majority of the time. Scruggs claimed she kept trying to call Devon because she wanted to leave, and Devon told her to just leave him if she did not want to stay. Scruggs ended up leaving Devon downtown because he did not want to leave.

22. Later that day, law enforcement met again with Scruggs, at her request. Law enforcement showed Scruggs the photo of Vaughn taken during the B&L arson, and asked Scruggs if she thought it was her boyfriend. Scruggs initially stated she did not know if that was him or not. After looking at the photo for a while, Scruggs stated the photo did “kind of” look like him, and that the hat and tattoo did look like Devon’s.

23. On September 3, 2020, ATF Special Agent Rick Hankins and DCI Special Agent Kevin Heimerl interviewed Kevin Vaughn. Investigators first made contact with Kevin Vaughn’s ex-wife at another location and she provided a current address for Devon Vaughn and Kevin Vaughn as 925 Arthur Avenue, Racine, WI.

24. Agent Hankins knocked on the front door of 925 Arthur Street and a male juvenile answered. Agent Hankins asked the juvenile if Devon was home and the juvenile said Devon had been home but was no longer home. While investigators were standing on the front porch, Kevin Vaughn (the father of the juvenile) arrived in a vehicle.

25. When asked, Kevin Vaughn stated that his nephew, Devon Vaughn, stays with him periodically. Specifically, Kevin said that Devon moves back and forth between Kevin’s house and Devon’s girlfriend’s house. Kevin said that Devon dated a girl named “Tab.” Kevin further said that Devon mainly sleeps on the couch in the front living room. Kevin also said Devon had stayed at 925 Arthur Avenue for 4-5 nights in a row.

26. When asked, Kevin Vaughn said Devon Vaughn’s cellphone number is (262) 234-1468. Kevin stated that he has seen Devon with two cellphones, but he only calls Devon at (262) 234-1468.

27. Agent Hankins informed Kevin Vaughn that investigators had learned that Devon Vaughn was out during the unrest in Kenosha. Kevin stated that he knew Devon and Tab were

out in Kenosha during the daytime. However, Kevin further said that if Devon was out in Kenosha at night then he must have missed work.

28. Devon Vaughn eventually learned of law enforcement's investigation, after which point Devon Vaughn contacted an ATF agent on September 7, 2020, using the telephone number of (262) 676-9514.

29. Law enforcement requested that legal process issue to Apple regarding the two known phone numbers of Devon Vaughn: (262) 676-9514 and (262) 234-1468. Law enforcement specifically requested that Apple identify any Apple IDs or Apple iCloud accounts associated with Devon Vaughn's known telephone numbers.

30. In its response to this same legal process, Apple indicated that the telephone number of (262) 234-1468 was indeed associated with the two Apple iCloud accounts identified in Paragraph 1 and Attachment A.

31. Based on the information above, and the technical information that follows, there is probable cause to believe that the information described in Attachment A contains evidence of violations of arson of commercial property, in violation of Title 18, United States Code, Section 844(i), as described in Attachment B.

INFORMATION REGARDING APPLE ID AND iCloud¹

32. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

33. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

- a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.
- b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.
- c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.
- d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user’s Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations.

¹ The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: “U.S. Law Enforcement Legal Process Guidelines,” available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; “Create and start using an Apple ID,” available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
 - f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
 - g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
 - h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.
34. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

35. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

36. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

37. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

38. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is

linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address (“MAC address”), the unique device identifier (“UDID”), and the serial number. In addition, information about a user’s computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user’s web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

39. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user’s photos and videos, iMessages, Short Message Service (“SMS”) and Multimedia Messaging Service (“MMS”) messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user’s instant messages on iCloud Drive. Some of this data is stored on Apple’s servers in an encrypted form but can nonetheless be decrypted by Apple.

40. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion. As described above, the historical location information and other records shows that Devon Vaughn traveled to Kenosha, Wisconsin on August 24, 2020.

41. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation. Based on the information described above, it is probable that communications, including instant messages, emails, voicemails, photos, videos, and call records, from Vaughn, including those before, during, and after the B and L Office Furniture arson, are likely to be contained in the records and information associated with Apple iCloud dtvon@icloud.com and dtv2017@icloud.com and any accounts associated with Devon Vaughn, along with evidence of any attempt to delete records and information relating to this investigation and Vaughn’s whereabouts before and after he traveled to Kenosha on August 24, 2020.

42. In addition, the user’s account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-

location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation. In the investigation of an arson during a riot, this information is all the more important to corroborate who is using the phone and participating in communications.

43. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

44. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation. In this case, it may also allow investigators to pursue other investigative leads.

45. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and

experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

46. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

47. Based on the forgoing, I request that the Court issue the proposed search warrant.

48. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

ATTACHMENT A

Matter No. 2020R00324

Property to Be Searched

This warrant applies to information associated with the Apple IDs and Apple iCloud accounts associated with the following information, that is stored at premises owned, maintained, controlled, or operated by Apple Inc., a company headquartered at Apple Inc., One Apple Park Way, Cupertino, California 95014.

Account 1:

- Name: Tyler Vaughn
- Email: dtv2017@icloud.com
- Phone: (262) 234-1468
 - Person ID: 17412011338
- Addresses: 327 Kenzie Ave. Racine, WI 53405

Account 2:

- Name: Dev Vaughn
- Email: dtvon@icloud.com
- Phone: (262) 234-1468
 - Person ID: 17429487926
- Address: 925 Author Ave. Racine, WI 53405

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

b. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers

(“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

c. The contents of all emails associated with the account from August 23, 2020 through the date this warrant issued, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the account from August 23, 2020 through the date this warrant issued, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

f. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and

query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

g. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

h. All records pertaining to the types of service used;

i. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

j. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within **14 DAYS** of issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence of violations of arson of commercial property, in violation of Title 18, United States Code, Section 844, involving Devon Vaughn since August 23, 2020, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Preparatory steps taken in furtherance of these crimes;
- b. Communications between Devon Vaughn and Tabitha Scruggs;
- c. Information about the protests, riots, and civil unrest in the Kenosha, Wisconsin area occurring between August 23, 2020 and the date this warrant issued;
- d. Use, possession, custody, or control of the phone numbers (262) 676-9514 and (262) 234-1468;
- e. Accelerants or ignitable liquids (such as gasoline, kerosene, or other petroleum distillates), glass bottles, ignition devices (such as an improvised wick or towel), heat sources, and ignition sources (such as a lighter or matches);
- f. Appearance, clothing, and identity of Devon Vaughn on August 24, 2020;
- g. B & L Office Furniture, located 1101 60th St. Kenosha, WI;
- h. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
- i. Any information related to motive, intent, or knowledge of the violations described above;
- j. Any information related to the concealment or destruction of evidence of the violations described above;
- k. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the account subscriber;
- l. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);
- m. Evidence indicating the subscriber's state of mind as it relates to the crime under investigation; and

- n. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.